IN THE CLAIMS

1-3. (Cancelled)

4. (Currently amended) A method comprising: ~~The method of claim 3, further comprising:~~

receiving node information for a node coupled to a computer network;

analyzing the received node information to identify a unique identifier;

selecting at least a security identified provided by an operating system of the node for [[as]] the unique identifier when the analysis indicates that the node information includes the security identifier;

selecting at least a serial number provided by a basic input output system of the node for [[as]] the unique identifier when the analysis indicates that the node information does not include the security identifier; ~~and~~

selecting at least a physical address for [[as]] the unique identifier when the analysis indicates that the node information does not include either of the security identifier and the serial number[[.]];

determining whether to issue an alarm indicating a network intrusion responsive to receiving the node information by comparing the unique identifier to a database;

automatically linking at least a portion of said node information to an existing database entry in the database and not issuing the alarm when the comparison indicates a tracked entity that corresponds to the node; and

issuing the alarm indicating the network intrusion and creating a new database entry when the comparison indicates that the node is a new entity.

5. (Currently amended) The method of claim [[1]] 4, ~~further comprising:~~

~~analyzing the node information to select the unique identifier;~~

wherein the ~~selected~~ unique identifier is not based solely on an ~~IP~~ Internet Protocol (IP) address such that the determination of whether the alarm is sent is independent of whether the node is subject to static or dynamic address assignment.

6. (Currently amended) The method of claim 5, wherein the unique identifier is a combination of [[a]] the physical address and a network address for the node.

7. (Currently amended) The method of claim [[1]] 4, wherein the unique identifier ~~that is compared to the database~~ includes a domain name associated with the node, a computer name associated with the node and one other value associated with the node.

8. (Currently amended) The method of claim 7, wherein the other value is a security identifier, a serial number or [[a]] the physical address.

9. (Currently amended) A method comprising: ~~The method of claim 8, further comprising:~~

receiving node information for a node coupled to a computer network;

selecting from the received node information ~~the~~ a security identifier for use in a unique identifier ~~for the other value~~ when the security identifier is available ~~included in the node information~~, and when the security identifier is not available, ~~included in the node information~~ selecting a substitute value for use in the unique identifier, the substitute value being at least one value selected from the group of a serial number, a physical address and another statically assigned value; ~~the serial number for the other value, and when neither of the security identifier and the serial number are included in node information selecting the physical address for the other value.~~

determining whether to issue an alarm indicating a network intrusion responsive to receiving the node information by comparing the unique identifier to a database;

automatically linking at least a portion of said node information to an existing database entry in the database and not issuing the alarm when the comparison indicates a tracked entity that corresponds to the node; and

issuing the alarm indicating the network intrusion and creating a new database entry when the comparison indicates that the node is a new entity.

10. (Currently amended) The method of claim [[1]] 9, wherein the unique identifier is a combination of the physical address and a network address for the node ~~said entity is a computer system running a particular operating system~~.

11. (Currently amended) The method of claim [[1]] 9, wherein said tracked entity is a user of said computer network.

12. (Currently amended) The method of claim [[1]] 9, wherein said tracked entity is a computer system.

13. (Previously presented) An apparatus comprising:

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

receive node information for a node coupled to a computer network;

analyze identifiers included in the received node information to select a value for comparing to a database that lists tracked entities;

determining whether the node corresponds to one of the tracked entities by comparing the selected value to the database;

when the node corresponds to one of the tracked entities, linking at least a portion of the received node information to an existing entry in the database; and

when the node does not correspond to one of the tracked entities, adding an entry for a new entity to the database and linking the node information to the new entry.

14. (Currently amended) The apparatus of claim 13 wherein the selected value is not based on an Internet Protocol (IP) address such that the node can be correlated to one of the tracked entities even when the node is subject to dynamic IP address assignment.

15. (Previously presented) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a security identifier is unavailable.

16. (Previously presented) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a serial number is unavailable.

17. (Previously presented) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a different preferred identifier is unavailable.

18. (Previously presented) The apparatus of claim 13 wherein the selected value is based on both a physical address and a network address when a different identifier is unavailable.

19. (Currently amended) The apparatus of claim 13 wherein the selected value is ~~either not a network address or is~~ a combination of the network address and a globally unique identifier.

20. (Previously presented) The apparatus of claim 13 wherein the selected value is not based on an IPv4 address such that the node can be correlated to one of the tracked entities even when the node is subject to dynamic IPv4 address assignment.

21. (Previously presented) The apparatus of claim 13 wherein the processors are further operable to:

select either a security identifier provided by an operating system of the node or a serial number provided by a basic input output system of the node for the value when the received node information includes either the security identifier or the serial number; and

select a physical address for the value when the received node information does not include either the security identifier or the serial number.

22. (Previously presented) The apparatus of claim 13 wherein the processors are further operable to trigger issuance of an intrusion alarm when the node does not correspond to one of the tracked entities.

23. (Currently amended) The apparatus of claim ~~22~~ 13 wherein issuance of a false alarm is avoided when the received node information is linked to an existing entry in the database.

24. (Previously presented) The apparatus of claim 13 wherein the processors are further operable to use adaptive scanning before determining whether to issue an alarm.

25. (Currently amended) A system, comprising ~~method for tracking entities in a computer network comprising~~:

means for receiving node information related to a node on said computer network;

means for analyzing the received node information to located a unique identifier that is able to uniquely identify ~~said~~ an entity associated with the node, the unique identifier being a value other than a network address for the node;

means for determining if a database entry exists by searching said database using multiple identifiers from said node information that are not able to individually uniquely identify said entity, if said node information does not include said unique identifier;

means for linking at least a portion of said node information to said entry if said entry exists; and

means for creating a new entry in said database for said entity if no entry exists for said entity, and linking at least the portion of said node information to said new entry.

26. (Currently amended) The system ~~method~~ of claim 25, wherein said multiple identifiers comprise a media access control (MAC) address.

27. (Currently amended) The system ~~method~~ of claim 26, wherein said multiple identifiers further comprise a computer name.

28. (Currently amended) The system ~~method~~ of Claim 27, wherein said multiple identifiers further comprise a domain name.

29. (Currently amended) The system ~~method~~ of Claim 28, wherein said multiple identifiers further comprise an operating system identifier.

30. (Currently amended) The system ~~method~~ of Claim 28, wherein said multiple identifiers comprise at least two of: a media access control (MAC) address, a computer name, a domain name, and an operating system identifier.

31. (Currently amended) The system ~~method~~ of Claim 25, wherein said unique identifier comprises a security identifier.

32. (Currently amended) The system ~~method~~ of Claim 25, wherein said unique identifier comprises a serial number.

33. (Currently amended) The system ~~method~~ of claim 25, further comprising:

means for returning an identifier for an entity in response to a request including a node identifier.

34. (Currently amended) The system ~~method~~ of Claim 25, further comprising:

means for returning identifiers for all nodes associated with an entity in response to a request including an entity identifier.

35. (Currently amended) The system ~~method~~ of Claim 25, further comprising:

means for returning node information in response to a request for said node information including a node identifier.

36-42. (cancelled)

43. (Previously presented) A system for tracking computer entities in a computer network, comprising:

a database storing therein entries related to entities in said computer network;

an engine coupled to said database, wherein said engine is operable to:

receive node information related to a node coupled to said computer network;

determine whether an entity associated with said node has been previously identified in said computer network;

link said node information to an existing entry for said entity in said database if said entity has been previously identified in said computer network; and

create a new entry for said entity in said database if said node has not been previously identified in said computer network and link said node information to said new database entry for said entity;

wherein said engine is further operable to determine if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not a unique identifier in said node information.

44. (Previously presented) The system for tracking entities in a computer network of claim 43, wherein said engine is further operable to determine if a computer name from said node information matches a computer name associated with said MAC address in said database.

45. (Previously presented) The system for tracking entities in a computer network of claim 43, wherein said engine is further operable to determine if a computer name from said

node information matches a computer name in said database and determine if a domain name from said node information matches a domain name associated with said computer name in said database.